

PUBLIC RELEASE AUTHORIZED



United States Air Force Scientific Advisory Board
Report on
Networking to Enable Coalition Operations
Volume 1: Executive Summary and Annotated Brief
[PR]

1 July 2004

DISTRIBUTION AUTHORIZED

In accordance with AFI 61-204, distribution statement A, this document is approved for public release; distribution is unlimited.
Approved for public release by SAF/PAX 23 Nov 04.

PUBLIC RELEASE AUTHORIZED

PUBLIC RELEASE AUTHORIZED

This report is a product of the United States Air Force Scientific Advisory Board Study Committee on *Networking to Enable Coalition Operations*. Statements, opinions, findings, recommendations, and conclusions contained in this report are those of the Study Committee and do not necessarily represent the official position of the United States Air Force, United States Department of Defense, or United States Government.

PUBLIC RELEASE AUTHORIZED

PUBLIC RELEASE AUTHORIZED



United States Air Force Scientific Advisory Board
Report on
Networking to Enable Coalition Operations
Volume 1: Executive Summary and Annotated Brief
[PR]

1 July 2004

DISTRIBUTION AUTHORIZED

In accordance with AFI 61-204, distribution statement A, this document is approved for public release; distribution is unlimited.
Approved for public release by SAF/PAX 23 Nov 04.

PUBLIC RELEASE AUTHORIZED

PUBLIC RELEASE AUTHORIZED

(This Page Intentionally Left Blank.)

PUBLIC RELEASE AUTHORIZED

Foreword

The US Air Force has begun migration toward a transformational network-enabled force. At the same time, collaboration with coalitions has become increasingly important in warfare for political, access and overflight, and operational capabilities reasons. However, new systems and technologies that enable effective networked operations are not always available or affordable to coalition partners. Adequate realistic training of U.S. forces and coalition partners is not always undertaken. Instituting more effective coalition net-centric operations will require the appropriate communications, including data links; collaboration with coalition partners in order to best take advantage of their capabilities; exploitation of network capabilities to compensate for inadequacies of participating systems; and the use of collaborative multi-level secure information interchange among coalition command centers. An evolutionary and affordable network-based collaborative planning and execution capability for both the U.S. and its coalition partners can be designed and implemented, which will, in turn, yield a more effective total coalition force in future operations.

This study addresses this challenge of more effective *Networking to Enable Coalition Operations* (NECO). The study was conducted in response to a request by the Secretary of the Air Force and the Chief of Staff of the Air Force.

In response to their direction, the NECO study team conducted an extensive set of visits to all major Air Force operating commands and key operations centers, and reviewed numerous briefings from Air Force, Joint and coalition organizations concerning current operations, systems, and procedures, as well as proposed future system and process improvements. The assistance of these organizations was essential to the completion of our effort. It was their involvement that guided the study team toward the findings, concepts, conclusions, and recommendations that comprise this study. The study team greatly appreciates the cooperation of these organizations, and acknowledges the valuable contributions their efforts made to this study.

The undersigned also wish to acknowledge the outstanding effort put forth by the Air Force Scientific Advisory Board Secretariat, the members of the NECO study team, the Study Executive Officers, and the Technical Writers in the preparation of this study – whatever value is found in this work is attributable to them.



Mr. Howard K. Schue
NECO Study Chairman



Dr. Peter R. Worch
NECO Study Vice Chairman

PUBLIC RELEASE AUTHORIZED

(This Page Intentionally Left Blank.)

PUBLIC RELEASE AUTHORIZED

Executive Summary

Introduction

In the past four decades, the United States has been the predominant force in peacekeeping, peacemaking, and combat operations in which it has participated. Two changes are now being experienced. First, post-Cold War contingencies and the Global War on Terrorism have illustrated the increasing importance of constructive coalition relations. Second, as U.S. Forces become more network-centric, effective integrated operations with coalition partners are becoming increasingly difficult and dependent upon the ability to share information electronically. In particular, the dynamic nature of air operations demands rapid transfer of data among the forces. However, security concerns prevent full (and often, even partial) access to our networks by others. While workarounds have been implemented, sometimes with excellent combat results, this limited access has impaired the ability of U.S. Forces to truly exploit the diverse capabilities of coalition partners and perhaps reduce U.S. Forces' operations tempo. This Study addresses the issue of networking for coalition air operations from policy, operational, and technical viewpoints. In fact, all three are at issue in the current operations architecture.

The Study members visited, or were briefed by, Air Force, Joint, foreign, and multi-national organizations. The following summarizes the information gathered, the conclusions expressed as a vision for the future, and some recommendations for Air Force action. Since the problem spans all Services, the nation's security and defense agencies, and its alliances, the solutions must include Joint- and Office of the Secretary of Defense (OSD)-level actions.

The Situation

The degree of collaboration that the U.S. has exercised with coalition partners in the planning and control of air operations has varied greatly depending on the country involved. Prior to recent operations in support of Operation Iraqi Freedom (OIF), allied participation in U.S.-led air operations had been oriented toward supplying augmenting forces. Some nations [e.g., North Atlantic Treaty Organization (NATO) members] have contributed key capabilities in short supply in the U.S. [e.g., Area of Responsibility (AOR)-specific intelligence]. Some nations have offered forces capable of executing specific portions of the Air Tasking Order (ATO). Other nations have offered forces not capable of independent action. In recent operations, select coalition partners have collaborated quite closely with U.S.-led air operations. However, even the most trusted coalition partners have had severe restrictions placed upon how, where, and when they were allowed to access U.S.-derived intelligence data and U.S. mission planning systems within the Combined Air Operations Center (CAOC) planning and execution processes.

U.S. Central Command Air Forces' (USCENTAF) experiences in bringing non-U.S. members into the Al Udeid CAOC during OIF are illustrative of the coalition challenges that must be addressed. For both Operation Enduring Freedom (OEF) (Afghanistan) and OIF in 2001-2004, U.S. Central Command (USCENTCOM) instituted a number of physically separate networks to support information exchange among different groups of coalition partners. As OEF began, USCENTCOM used a network known as the Combined Enterprise Regional Information Exchange System¹ (CENTRIXS) as its Command and

¹ CENTRIXS (Combined Enterprise Regional Information Exchange System): A collection of systems, each of which is intended to facilitate multi-national information sharing in a particular coalition environment

Control Backbone. As operations expanded, a more robust network was required. Developing even more robust versions of CENTRIXS proved unsatisfactory. Eventually, prior to OIF, USCENTCOM transitioned to the U.S.-only SECRET Internet Protocol Router Network (SIPRNET) backbone. This action resulted in a primarily U.S.-only planning activity with very limited coalition participation. As OIF's "major combat" activity level declined, authority to operate on SIPRNET expired and the coalition returned to the CENTRIXS backbone.

The challenges in achieving effective coalition air operations are significant. Policymakers are reluctant to change policy because, in part, they perceive that technology is not available to provide acceptable automated protection of classified information. Technologists believe technical solutions are precluded by policy decisions. This leaves operators caught in between. In fact, policy, technology, and operations are interdependent, and the solution will only come by diligent and integrated efforts in all three camps.

The Concept of Operations (CONOPS) Vision

Coalition-based operations are planned and executed by human teams. To function in a high performance manner, teams must have accepted leadership and clear roles and responsibilities. They need well-crafted and clear rules of engagement, excellent communication, and they must be grounded in experience and trust. While the experience of individual team members may be assumed, the experience of the team itself and the trust among the team members is problematic because of the likely "pick-up" nature of coalition-based teams. In turn, they are influenced by the cultural nuances of the constituent countries involved in the coalition.

We have established that constructive coalition relations are an important instrument of foreign policy as well as having potential for helpful force contribution. It is essential, therefore, that both planning and execution as accomplished in the CAOC be done in a fashion that emphasizes "team coalition" and minimizes "national separation." The sharing, based on the commander's intent, of information derived from individual country assets (strategic or tactical), and seamless integrating of that knowledge with information from sources committed to, and controlled by, the coalition is a great challenge to team relations. The lead nation (which may not be the U.S.) must assume responsibility for establishing the parameters and safeguards for information sharing (i.e., who, when, and how will participants get access, what happens if participants violate access procedures). Along with policy responsibilities, the lead nation must be responsible for designing and providing hardware capable of sharing information in a coalition environment (i.e., the lead nation must demonstrate its intention to share by providing a network that is capable of sharing). Design must be coalition-centric and, in order to be effective, must exist in peacetime to include appropriate training. Previous operations have been hampered by the use of non-interoperable nation-centric hardware.

The effectiveness/value of the coalition network will rest on the quality of data housed on the system. As such, participants must create operationally-pertinent data sources which are compatible with the coalition network and coalition-releasable. Participants will still have the ability to communicate with their specific leadership via a "National Network" (every Nation will have its own architecture).

Realizing this vision will require several actions to establish and implement standards and to develop and integrate technologies.:

Standards – Since coalitions are likely to be fluid from situation to situation and will need to be assembled rapidly for each new operation, commonly understood standards will be critical for success. They will be needed to support interoperability with a potentially wide range of partners and to facilitate rapid assembly and deployment of the network infrastructure for a new coalition. Fortunately, the commercial information technology market provides much of the capability for basic networking and collaboration. What the commercial world does not provide, and what the government needs to develop are standard security-related solutions.

Technology – Each group of nations that wishes to share information with each other while protecting that information from others requires the creation of a unique security domain to segregate their information. To transfer information between security domains requires a controlled interface commonly called a cross-domain solution or guard. Research and development (R&D) initiatives should focus on several needed technologies:

- Rule-based access control;
- Metadata-derived releasability;
- Cross-domain Public Key Infrastructure (PKI);
- Cross-domain collaboration and discovery; and
- Cross-domain access and Multi-Level Security.

Data Management

Information release in the network of the future should be based on the concept of *metadata-derived releasability (MDR)*. In this approach, releasability will be determined based on the content of the information, how it is to be used, and by whom, rather than its classification level alone. Elements in the databases will have meta-tags that describe their content, based on a standardized ontology of metadata tags. Automated rule-based foreign disclosure guards are created that use these tags to determine what may be moved from national networks into the coalition network and dynamically update the coalition network as information in national networks changes. Access to information will be determined not simply by the nationality of the intended recipient, but also by the *role* that a participant plays and the *content* of the information, again using rule-based guards that examine the meta-tags to determine releasability of coalition network information to individual participants.

System Evolution

The Study's vision for the evolution to an objective system evolves the system through three spirals. Spiral 0 is a construct which acknowledges today's ongoing efforts to deal with coalition issues. Recent experiences have stimulated initiatives to achieve certain near-term incremental improvements. Spiral 1 pursues an end state that is workable and achievable within the technology limits imposed by approaches that use network boundaries as the mechanism for controlling information access. Spiral 2 is a "next level" of performance that can be achieved when rule-based information and MDR become available.

Recommendations

1. Policy: Advocate security releasability policies that remove impediments to network-enabled coalition operations. A consistent approach to "need-to-share" should be the objective for handling of

information in coalition operations. A mindset shift from risk-averse policy and culture is essential, and creation and implementation of a coalition releasable classification system can facilitate the concept. Within the Air Force, streamlined approval processes based on commander's intent can improve air operations with coalition partners.

2. Training: Establish a comprehensive coalition training and exercise program that fully integrates coalition partner nations on a routine basis. Exercises with coalition nations should reflect combat realities, rather than the current procedure of "dumbing down" to accommodate current policy and culture constraints. Moreover, such exercises should take full advantage of our partners' unique operational capabilities so as to train their forces as well as our own.

3. Operational Capabilities: Designate the "CAOC as a weapon system." Designating the CAOC as a weapon system establishes it as a major focus program within the Air Force, thus assuring a formal architecture, continuing configuration management, comprehensive training, and a long term plan for capabilities enhancement. Putting the "C" in CAOC should be reflected by coalition warfare becoming a key performance parameter (KPP) in future requirements documents and system development.

4. Technology: Aggressively promote and influence multi-agency technology developments essential to effective coalition operations. Though many technologies for enhanced security management are available, some other needed technologies are being addressed in various activities and agencies, while yet others are not receiving adequate attention. The Air Force should take the initiative to assure efforts are coordinated and complementary.

5. Systems: Establish a distributed coalition network environment that will enable and encourage nations to develop interoperable command and control systems. The study suggests a spiral improvement in capabilities, building on current CENTRIXS and Intelligence Community System for Information Sharing² (ICSIS) architectures with cross-domain security technology developments. In the longer term, the goal is a metadata derived releasability concept based on content tagging of information elements enabling automated access according to nation, rule and individual role.

Summary

The Study concludes that technology, policy, and process improvements are essential to effective coalition air operations. The Air Force can take unilateral action to further developments, designate the CAOC as a weapon system, foster demonstrations and experiments to explore CAOC solutions, and improve training and exercises.

² ICSIS (Intelligence Community System for Information Sharing): A certified and accredited system developed under the sponsorship of the IC-CIO implementing an agreed-to set of services that facilitate information sharing. It is currently a single domain system but is evolving to include cross-domain services



Air Force Scientific Advisory Board

Integrity - Service - Excellence

Networking to Enable Coalition Operations Study Outbriefing



U.S. AIR FORCE

**Mr. Howard Schue – Chair
Dr. Pete Worch – Vice Chair**

1 July 2004

DISTRIBUTION AUTHORIZED

In accordance with DODD 5230.24, distribution statement A, this document is approved for public release; distribution is unlimited.





The Need for Coalitions

- Coalition relations are an important instrument of foreign policy
- Coalition warfare is becoming increasingly important to the nation
 - ✓ The U.S. will almost always conduct operations as a member of a coalition of the willing, most often as the lead
 - ✓ The Global War on Terrorism will mandate diverse contributions and political support of non-traditional coalition partners
 - ✓ Coalition partners sometimes have capabilities the U.S. does not
 - ✓ Future force reductions may increase dependence on coalitions
 - ✓ Coalition support is essential for achieving the peace after combat operations
- In today's world, information is dramatically more important; Networks are the mechanism for sharing information
- Effective networking is based on trust developed through coalition training, exercises, and operations
- More effective use of coalition and treaty partners' capabilities will reduce U.S. ops tempo and improve effectiveness

Integrity - Service - Excellence

2

We perceive coalitions as becoming increasingly vitally important to the nation. Coalitions, of course, are political creatures and are largely determined by our political seniors and in turn issued to the Air Force. It becomes the Air Force's responsibility to determine how these coalitions will be employed to pursue combat mission objectives. Coalition partners also may have capabilities that, despite our proud history, we may not have. Cases in point are localized, detailed Human Intelligence information and certain Combat Search and Rescue and Electronic Warfare capabilities that other nations have to a degree that we do not. We believe the global war on terrorism that we are currently pursuing will mandate increasingly different kinds of combat operations. Therefore, we will find ourselves in coalitions not only with our traditional partners, but also non-traditional partners. Future force reductions that the Air Force might encounter may also have the effect of increasing our reliance, or perhaps dependence, on the capabilities of our coalition partners. In addition, as we are learning everyday in Iraq, even if we do not need a coalition partner to successfully execute an operation or perform a mission, they may be essential for achieving and maintaining a constructive peace after combat is over. Our conclusion is that the U.S., and therefore the Air Force, will almost always fight or conduct future operations in a coalition. We will most often be in the lead but not always, so our thinking about coalitions must take into account the circumstance both where we may be the only member of the coalition, i.e., a coalition of one, and also where we are not in the lead and must follow the direction of another commander. The bottom line to all of this is that the effective use of our coalition partners through enhanced networking will enable a higher level of effectiveness and reduce the operations tempo of U.S. troops. So, we see the need for coalitions and effective networking of coalitions as vitally important to the Air Force.



NECO Study Charter


- Consider approaches for a **networked collaborative process**, and the systems that support it, to provide more effective coalition forces for future operations
- Suggest **technology releasability guidelines** for potential coalition partners
- Develop **guidelines for Operational Concepts** for a networked coalition
- Identify a set of **high payoff opportunities** for enhancing interoperability while maintaining a proper level of security among component systems
- **Propose a roadmap** for integrating or federating US and ally/coalition partner systems into a net-centric system-of-systems to enhance collaboration

Integrity - Service - Excellence

3


An abridged version of the Study's Terms of Reference is shown here. The full version is provided in Appendix A.

We were charged with looking at policy, technology, and process in order to examine approaches for improving the networked collaborative process that must take place between the U.S. and its coalition partners to improve the effectiveness of the entire coalition force in future operations. From this, we developed recommendations and a roadmap.


U.S. AIR FORCE

The Challenges

(Bottom Line Up Front)



- **Coalition warfare is a Joint problem, but neither Joint activities nor the Air Force have assigned a high priority (e.g., funding, policy, focus) to improving networking to support coalition operations**
- **Currently, AOCs use a SIPRNET (US Secret network) baseline, which, in effect, excludes coalition partner participation except under specific circumstances**
- **Technologists blame policy; Policy makers blame technology limitations; ... And the operators use “process workarounds” to compensate**
- **Many coalition-compatible network improvement initiatives are underway... but they are disjointed and sometimes redundant or even conflicting**



Integrity - Service - Excellence

4

We offer you the bottom line up front from the standpoint of the challenges that the U.S. and the Air Force face in this circumstance. Foremost among them is that the problem of coalition networking is not inherently an Air Force problem. It is inherently a joint and coalition problem; however, we found in our searches, little joint activity or coordinated Air Force activity toward the end of achieving high-priority movement toward effective coalition networking.

Worse, today we operate our Air Operations Centers (AOCs) on the U.S. SIPRNET. However, information on that network is not limited to DoD activities but also includes very sensitive SECRET level data from other cabinet level agencies, and so agencies in addition to DoD have control over network access. Concern for protection of their data has had the effect of limiting coalition partner access to the SIPRNET. It is only under very specific and carefully thought through circumstances that we allow any coalition partner access to this SIPRNET. Today, we find the technologists pointing to policy as the challenge and the policy maker naturally blames technology limitations. Multi-level security, for example, has been on the horizon for decades. Meanwhile, our allies are not fully included. In practice, the operator is left to address the combat mission with workarounds to compensate for shortfalls in systems, processes, and releasability protocols in the interest of mission. In fact, it is the performance of these outstanding men and women who prosecute our combat operations that have resulted in the success of coalition operations to date, not necessarily the system's policy and protocols that underlie them. They succeed in spite of the policy and technology limitations of the systems provided to them to plan and execute combat operations.

We also found that many coalition compatible network improvements are already underway, but in the main they are disjointed and sometimes redundant or even conflicting. This, then, is how we perceive the current situation's challenges.



The Solutions

(Bottom Line Up Front)

➤ **The Air Force should make “coalition warfare” – that is, fighting as a coalition – an integral element of every activity**

- ✓ **Designate “CAOC as a weapon system”**
- ✓ **Develop needed technologies, coordinated with Joint and coalition efforts**
- ✓ **Use experiments to validate and refine technologies, policies, and procedures for coalition operations**
- ✓ **“Train as you will fight” -- in coalitions**

➤ **The Air Force should take every opportunity and venue to encourage action at the Joint level (OSD, JCS, DISA, IC)**

- ✓ **Establish an appropriate priority for coalition networking and require a coalition key performance parameter for all net-centric programs**
- ✓ **Put appropriate budget and people resources on the problem**
- ✓ **Focus, consolidate, and align efforts in both policy and technology**

Integrity - Service - Excellence



5

By way of solutions we suggest two major thrusts.



For that part of the problem that is not the Air Force's, the Air Force should take every opportunity to advocate and encourage action at the joint level to move toward increased and more effective coalition networking. We suggest that the Air Force work to establish an appropriate priority throughout the joint community for coalition networking and insert KPPs into all net-centric warfare system programs to insure network friendliness for coalition operations. We also suggest an effort to advocate to OSD and Joint levels the allocation of sufficient resources – both in dollars and people – to the problem. There needs to be an overt effort to focus, consolidate, and align efforts which are somewhat disjointed. If we do this properly we may in fact be able to save money over what is being spent today and make more aggressive progress.

Second, within the Air Force, the Air Force should make fighting as a member of a coalition an important priority for every activity. We should acknowledge that we will fight as a coalition in the future, put the “C” in the “AOC weapon system,” and in fact make the CAOC a weapon system.

In order to accomplish this, we must develop some technologies that are not currently available as well as improve policies and releasability protocols. We believe these initiatives should be done in collaboration with our likely coalition partners. Finally, as we have learned again and again, we need to train as we will fight – in coalitions.



 	
<h2 style="text-align: center;">Study Team</h2>	
<div style="display: flex; justify-content: space-between;"> <div style="width: 60%;"> <p style="text-align: center;">STUDY LEADERSHIP Mr. Howard Schue, Chair Dr. Pete Worch, Vice Chair Dr. Alex Levis, Sr Civ Participant Brig Gen Bill Holland, USAF, GO Participant</p> </div> <div style="width: 35%;"> <p style="text-align: center;">STUDY MANAGEMENT Maj Chris Berg, USAF, Proj Mngr Maj Rob Renfro, USAF, Tech Writer Mr. Paul Hazell, Tech Editor</p> </div> </div>	
<p style="text-align: center;">REQUIREMENTS, OPERATIONAL CONCEPTS, OPERATIONAL ARCHITECTURES PANEL</p> <p style="text-align: center;">Maj Gen (Ret) John Hawley, USAF, Panel Chair</p> <p style="text-align: center;"> Mr. Tim Bonds Lt Gen (Ret) Lincoln Faurer, USAF Dr. Janet Fender (Civilian Participant) Maj Gen (Ret) George Harrison, USAF Maj Mike Walker, USAFR, Exec Officer Maj Helen Meisenhelder, USAF, Tech Writer </p>	<p style="text-align: center;">TECHNOLOGY, TECHNICAL ARCHITECTURES, ACQUISITION PANEL</p> <p style="text-align: center;">Dr. Llewellyn "Doc" Dougherty, Panel Chair</p> <p style="text-align: center;"> Mr. Ed Brady Mr. Scott Fouse Maj Gen (Ret) Eric Nelson, USAF Dr. Bill Swartout Dr. Lionel Tiger Capt Eve Burke, USAF, Exec Officer Maj Jeff Humphries, USAF, Tech Writer </p>
<p style="text-align: center;">ROADMAP AND IMPLEMENTATION PANEL</p> <p style="text-align: center;">Mr. Thomas "Skip" Saunders, Panel Chair</p> <p style="text-align: center;"> Dr. Ron Fuchs Dr. J.B. Peterson Lt Gen (Ret) Steve Plummer, USAF Dr. Bob Selden Mr. Phil Soucy Capt Mike Bucher, USAF, Exec Officer Maj Tim Landvogt, USAF, Tech Writer Mr. Mickey Schmidt, Multimedia </p>	<p style="text-align: center;">STANDARDS, RELEASABILITY, LANGUAGE, SECURITY PANEL</p> <p style="text-align: center;">Dr. Lou Metzger, Panel Chair</p> <p style="text-align: center;"> Maj Gen (Ret) John Casciano, USAF Dr. Steve Cross Dr. Ray O. Johnson Mr. Jim Shields Dr. Greg Zacharias Maj Ronjon Annaballi, USAF, Exec Officer Capt Cicely Levingston, USAF, Tech Writer </p>

We were blessed with an outstanding team of Scientific Advisory Board members, augmented by some consultants with talents unique to our study topic. Our Requirements Panel was led by Major General John Hawley, USAF (ret) and former Commander of the Air Force Command and Control, Intelligence, Surveillance, and Reconnaissance Center (AFC2ISRC), which has been and is intimately involved in the AOC networking process. Our other panels were all led by veterans of the 2003 Scientific Advisory Board study on "Technology for Machine-to-Machine Intelligence, Surveillance, and Reconnaissance Integration" (the MTM study), the conclusions and recommendations of which form the basis for much of our approach to the coalition networking problem.

  <h2 style="text-align: center;">Visits and Briefings</h2>		
U.S. AIR FORCE		
<u>COCOMs & Regional Commands</u>	<u>Headquarters Air Force</u>	<u>Department of State</u>
USEUCOM & USAFE	AF/CV	PM/RSAT
USPACOM & PACAF	AF-CIO	<u>Intelligence Community</u>
USSOUTHCOM & JIATF-S	AF/XO	DIA
USCENTCOM & CENTAF	AF/XOR	NSA
(MacDill, Shaw, Al Udeid)	AF/XIC	NRO
USNORTHCOM & NORAD	SAF/IAPD	IC-CIO
USJFCOM	AFC2ISRC	
USFK	Task Force Enduring Look	<u>Foreign Governments and NATO</u>
	<u>Functional MAJCOMs</u>	UK RAF Strike Command
<u>Department of Defense</u>	ACC/CC	UK (RED FLAG)
USD(P) – ISP (NDP)	AFMC/CC	Singapore (RED FLAG)
ASD/NII	AFSPC/CV	Denmark (RED FLAG)
JCS J6	AFSOC (point paper)	Spain (USCENTCOM)
DOD Force Transformation	<u>CAFs and Other Air Forces</u>	Australian DOD & DSTO
DISA	16 th AF (Aviano AB)	Sweden MOD
DSAWG	32 nd AOG (Ramstein AB)	Defense Attaché Office of Chile
<u>Department of Homeland Security</u>	Air Warfare Center	Defense Attaché Office of Ghana
USCG	RED FLAG	Defense Attaché Office of India
	BLUE FLAG	Defense Attaché Office of Australia
	DMOC (VIRTUAL FLAG)	NATO ACT
	AFRL	NATO ACO
	ESC	NATO NC3A
		NATO ACCS
<i>Integrity - Service - Excellence</i>		

We heard many important briefings and visited command and operational activities from the Arabian Gulf to the Pacific.

The Terms of Reference directed that we limit the scope of potential allies that we worked with, and the lower right portion of the chart shows the potential allies that we chose. Basically, we considered candidate participants in two dimensions – first, their Willingness to work with the U.S as a coalition partner, and second, their Ability to contribute in a sophisticated networked environment. These nations spanned the spectrum in these two dimensions, and were very helpful in providing insights to the Study Team on their perspectives on coalition networking.



Key Terms

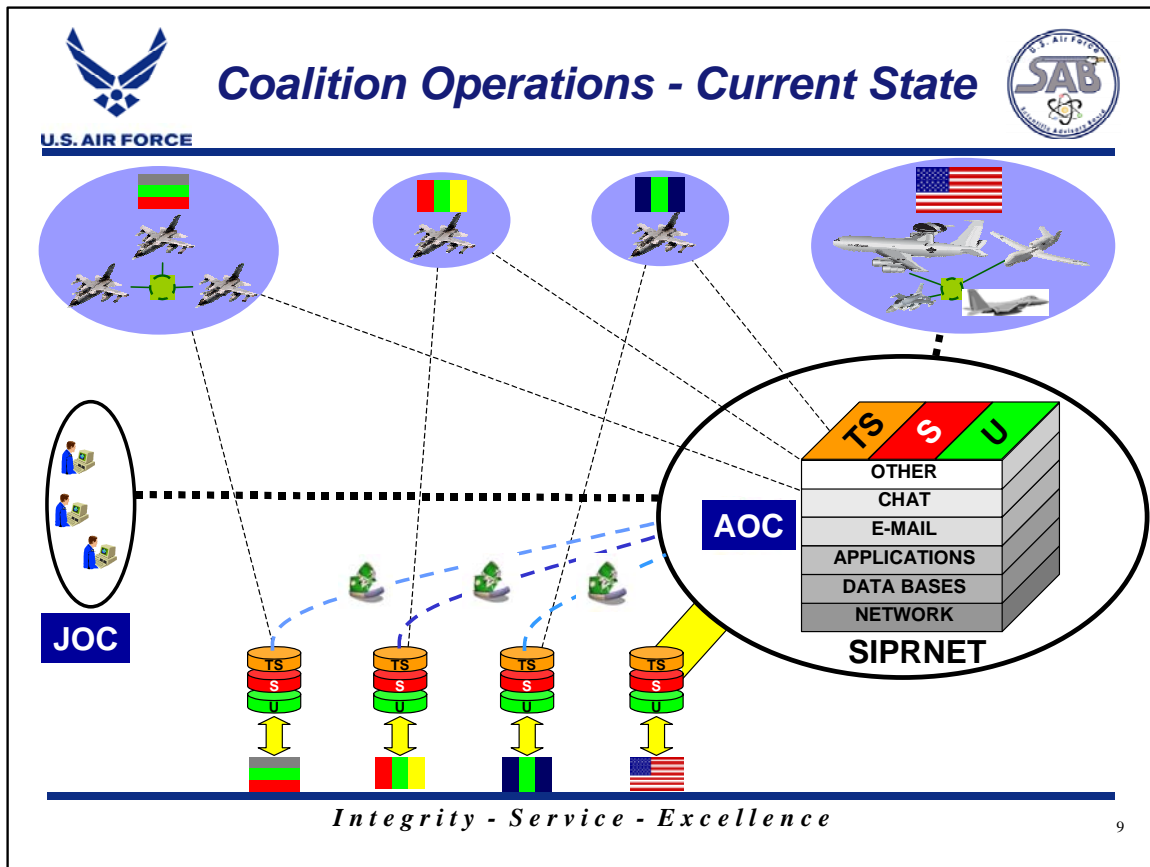
- **Networking:** A set of functional capabilities that facilitate communication and collaboration between interconnected groups and/or systems
- **Multi-Level Security (MLS):** Processing and transporting data of different security levels on a single processor and/or communications system
- **Multiple Security Levels (MSL):** Processing and transporting data of different security levels, with each level on a separate processor and communications system
- **Metadata Derived Releasability (MDR):** A concept for content-based tagging of information elements that would enable automated policy-based access

Integrity - Service - Excellence

8

Key terms that we will use throughout the report are as follows: *Networking*, which is in our title, means many things to many people. For us, it means a set of functional capabilities that facilitate communication and collaboration between whoever is connected to the network. *Multi-Level Security* means processing and transporting data of different security levels across a single processor or communication system, in contrast to *Multiple Security Levels* where data at different security levels are allocated to different networks or computers. These are two fundamentally different architectural philosophies. Building and operating acceptable Multi-Level Security systems, although deemed a desirable objective, are by-and-large beyond our technical capabilities today.



We now coin a new term: *Metadata-Derived Releasability* (MDR). This concept builds on ideas under development and to be demonstrated in the Content Based Information Security (CBIS) Advanced Concept Technology Demonstration. The key idea behind MDR is to tag individual pieces of data with metadata, that is, tags that describe the data in terms of its content, context, and structure. We then use rules to examine the metadata and direct the associated information to its destination based on the role and level of trust assigned to the recipient. This concept is important because it allows us to break away from network and data access that is based solely on the security level of the information, a paradigm that is too coarse-grained. It allows us to grant access selectively to individuals who are trusted and need particular pieces of information to perform their assigned roles effectively without granting them access to too much information.



This is a model of what the current system architecture looks like. We start with an AOC that is made up of a base network which, in this case, is SIPRNET. There are information databases on that network. There are applications, like targeting applications, which are particular to the mission at hand, and then there are collaborative tools like email and chat, and perhaps other tools as well on this network. Each network layer has its own security levels for data that are passing through these tools and each of them has protocols for handling the data. This is the multiple functionality we spoke of earlier that makes up networking in the AOC.

The AOC has the obligation of talking both to higher joint headquarters and also back to headquarters in the U.S.. All our other coalition partners have, notionally, the same sort of situation. They have their own classes of data (although they may not be as we call them), some of which they are willing to release to our coalition or to us, and some which they are not. They also have the responsibility of talking back to their own higher headquarters in their own countries.

Current barriers to information sharing results in the problematic reliance upon manual mechanisms (“sneakernets”) to move data back and forth between these various repositories, since our systems do not facilitate automated machine-to-machine transfer across security domains. The “sneakernet” is inefficient, slow, and incomplete.



What the Warfighter Wants...

- **Every coalition member has access to the data they need to do their mission**
- **Coalition members are confident that the information they share will only be disseminated to the extent needed to support the mission**
- **Coalition members are able to collaborate with one another in real-time over secure systems (and, where appropriate, fill positions in the CAOC Weapon System)**

Integrity - Service - Excellence



10

Moving on from the current situation to a discussion of the desired end state, we ask: Where would we like to go? Below (and in the above slide) is a statement that Major General Bob Elder made to us during our Summer Session and we think it is a good end state.

First, we would like to have every coalition member have access to the data they need to do the mission assigned to them. They do not need any more data than that, but conversely they do not need any less either.

Second, coalition members need to be confident that the information they share will only be disseminated to the extent needed to support the mission, so that their sensitive information is only used to prosecute the mission appropriately and is not used for other perhaps more nefarious purposes.

Last, coalition members also need to be able to collaborate with one another in real time over secure systems using adequate functionality to allow, facilitate and enable effective planning and execution. At the direction of the combat Commander, coalition members also need to fill work positions in a true CAOC weapon system, based on the Commander's judgment with respect to their role, nationality, and particular CAOC responsibilities.



CONOPS Vision

- Coalition operations are organized and commanded by a lead nation or organization
- Enhanced coalition networking enables full exploitation of coalition partners' warfighting capabilities
- Information access is granted by the Coalition Forces Commander based on assigned roles and responsibilities
- Categories of "Coalition Releasable" classified information are created and used by coalition members according to their roles
- Coalition forces agree upon and use established standards and processes for coalition operations
- Participating coalition parties provide coalition-releasable, coalition network compatible data sources
- Likely lead nations or organizations ensure adequate training and rehearsal

Integrity - Service - Excellence


12

Here is a broad CONOPS vision for how operations might be conducted under the desired end state. We see enhanced coalition networking capabilities that enable full exploitation of our coalition partners' warfighting capabilities, thereby limiting the stress on our own capabilities.


Coalition operations will be organized and commanded by a lead nation or organization, most likely the U.S., but not always. New categories of "coalition releasable" classified information will be used effectively by coalition members according to their roles and responsibilities as defined and determined by the coalition forces Commander. This is an important change from where we are today, where network access (or lack thereof) determines the degree to which we are able to collaboratively plan.

Coalition forces will be expected to establish and then use standards and processes for coalition operations.

Participating coalition parties must be willing to share coalition releasable versions of their data and put their coalition releasable information into the coalition dataset. Unless the coalition databases are populated with the information necessary to do true collaborative coalition planning and execution, we will fail here. So there is not only a need for collaboration on processes and systems there is also a need for collaboration on the insertion of appropriate levels of data. Finally, our assertion is that in order to make this a success, lead nations need to oversee the training and exercises, and rehearsal of these planning processes so that they are conducted in the same manner in which we intend them to be used in the fight.



Concept for Future Coalition Operations Security/Releasability Policy



U.S. AIR FORCE

- **Better balance between need-to-share and valid concerns for information protection**
- **Explicit, computer understandable representation of policy (i.e., releasability rules)**
- **Data ontology/schema agreements must be forged within communities of interest, including most likely coalition partners**
- **Policies and processes that require write-to-share (e.g., build on tearline concept)**
- **Evolved Foreign Disclosure Officer (FDO) function**
 - ✓ **Near-term: better trained, better tools, expanded role**
 - ✓ **Far-term: automated, rule-based information release**
- **Coalition toolkit of cross-domain security solutions whose application can be readily accredited by U.S. and its partners**

Integrity - Service - Excellence

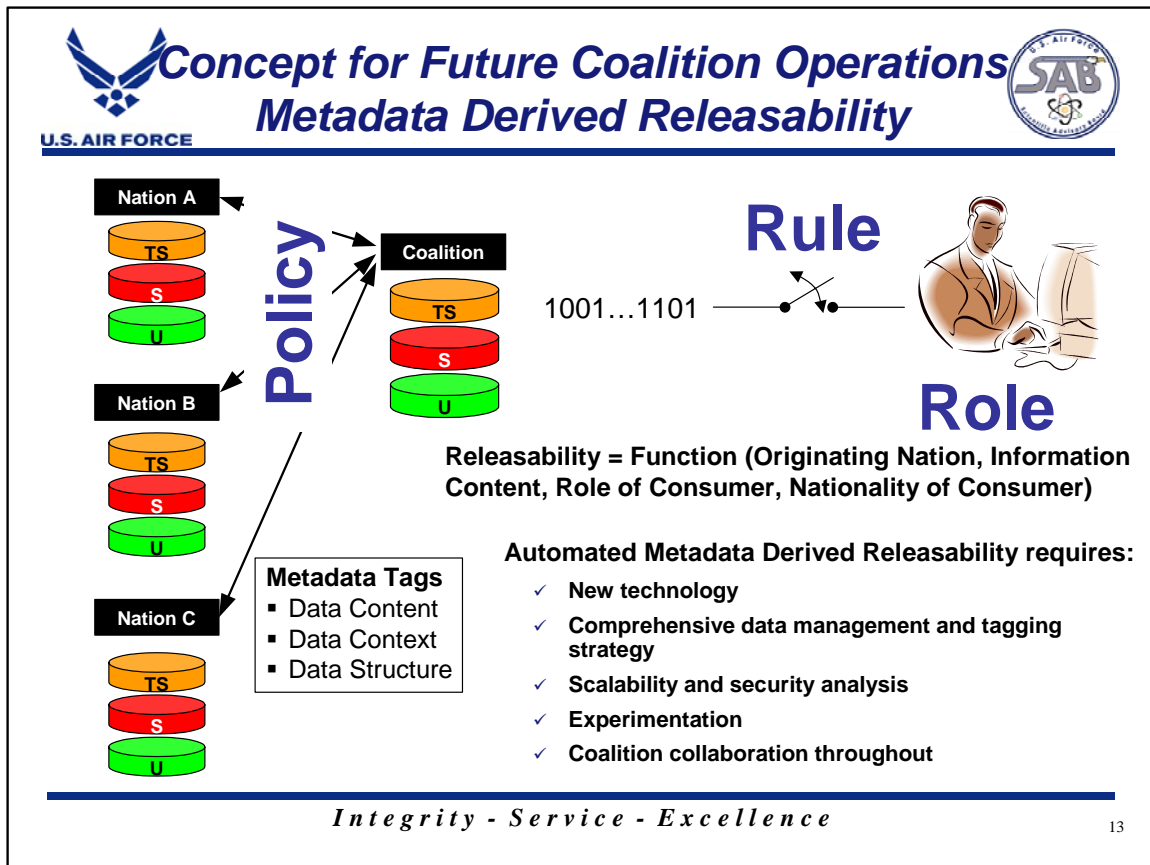
13

Coalition security and releasability policy must change. The balance between the need to know and the need to share must shift from the intense desire to protect our information toward a desire to share our information with those who have a valid need for it while providing adequate protection through risk management approaches. Explicit, computer-understandable, and implementable representations of policy, based on Commander's intent, must be developed to aid in releasability among coalition partners. This will require broad participation by U.S. defense and security agencies. In addition, development and validation of data ontologies and schema must also be forged with our most likely partners before operations begin.

We also need policies and procedures that deal with the handling of classified information to enable information sharing. One example is "tearline" approach to implementing the write-to-share practice being mandated within the IC. Here, an analyst, when creating classified material, breaks the document up into sections which are classified at different security levels. This allows the users to figuratively tear off only the sections that are appropriate to their security level.

We also need to revamp the functions of our Foreign Disclosure Officers (FDOs). Today's Foreign Disclosure Officers act as a manual cross-domain security guard. They serve as a mechanism for releasing data to our foreign partners. This is overloading the FDO workforce. In the near term, the FDOs need better training, better tools, and greater empowerment, particularly with respect to releasability of information originated by DoD organizations other than their own, and the process by which the NOFORN caveat (which directs that information not be disseminated to any foreigners) is applied to information. In the far term, we believe that many of the routine functions currently accomplished manually by FDOs can be handled with automated machine-to-machine rule-based decision-making and implementation.

Finally, we need to create a toolkit of specific security releasability approaches and a set of blueprints for their integration, which are pre-approved for application as cross-domain security solutions. Pre-approval means that accreditation for use in a particular coalition scenario can be quickly accomplished, since the solution is not being newly created from the ground up. Success in creating such a toolkit will require agreements to be forged across DoD and the IC as well as with our technically sophisticated, likely coalition partners. Stakeholders must be convinced that this toolkit is compatible with their national policies and that it securely implements them. The toolkit also needs to be compatible with multinational CENTRIXS-type coalition network approaches and be aimed at enabling in the end state a true, multi-level secure collaborative process where coalition partners can participate according to their role.



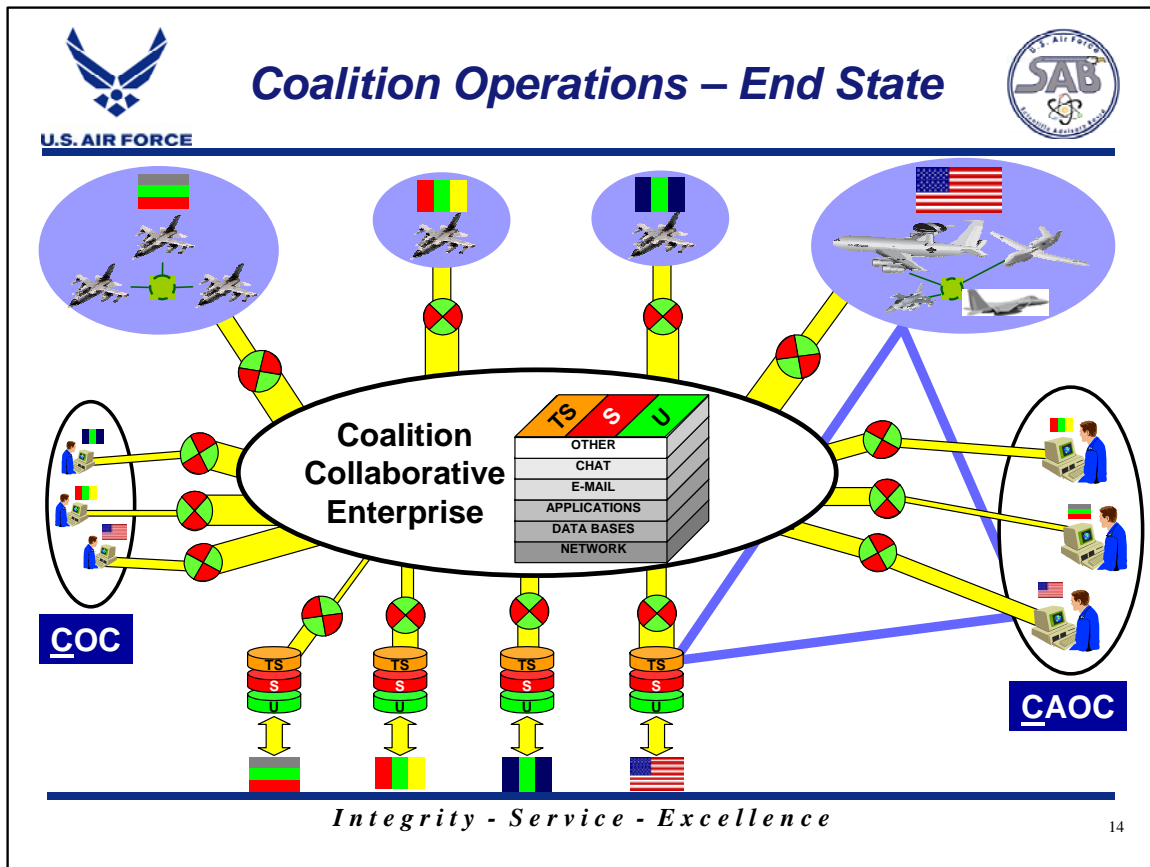
This model explains the concept of Metadata-Derived Releasability.

The left hand side represents several nations, each of which has its own information and its own classification levels, some of which it may choose to release to the coalition and some of which it may not. In the end state, each nation would tag its data with “metadata” which would provide, digitally, the information on the content, context, structure, and originating nation of the data, as well as other pertinent descriptions.

The data are then made available to the coalition via policy-based rules which use the metadata to make decisions about what data is released to the coalition database.

This information is further distributed to workers at the CAOC and other locations through a series of rules that automate the Commander’s intent and pre-arranged security agreements, via computerized decision making based on the metadata, the role for which the information is to be used, and the nationality of the person or persons who are filling that role.

Thus, an individual assigned by the Commander to a particular role in the CAOC would have access to the data he or she needs from the coalition database in order to accomplish his or her mission. This requires much change – technology needs to be developed to realize this concept, and policy and practice (and training) must enable it. The goal is to have the Commander’s intent and national policies reflected in an efficient machine-to-machine implementation of who sees what information to accomplish which roles in the CAOC.



This is a pictograph of our hoped-for end state vision. The key ingredient is the advent of MDR technology. That technology, represented by the “valve” symbol on the picture, allows information from the coalition to be appropriately metered to the individual person. The resulting collaborative enterprise can concentrate on information management and mission effectiveness rather than network administration or data acquisition issues. Implementation of this vision will entail having metadata data tags on information and the functionality necessary to properly distribute the data to users so that they can do truly collaborative planning. Operations centers will be staffed by coalition members, in accordance with the decision of the Coalition Commander, and with information access in accordance with their role. Communications to other member nations, higher headquarters, and tactical assets will likewise be controlled via MDR. Our vision of the future enables collaborative operations using data appropriately accessed by need and role as opposed to network access.



There are three additional points that need to be made about this end state, shown notionally in the diagram by the solid blue lines:

- This end state concept does not preclude the existence and use of separate U.S.-only networks (and coalition partner-only networks) to handle more sensitive national data and communications that are not shared with the coalition;
- This end state concept does not preclude effective operations if there is no coalition; that is, if the U.S. operates as a “coalition of one.” In fact, even in this circumstance, operations are significantly enhanced since data are distributed in accordance with individual need based on a U.S. service member’s Commander-assigned role; and

PUBLIC RELEASE AUTHORIZED

- This end state concept, while applied to the CAOC, or the operational level of operations in this example, is extensible to other levels of command and control, both lower and higher.

PUBLIC RELEASE AUTHORIZED



Concept for Future Coalition Operations Technologies

- **Trusted cross-domain security solutions are crucial to enabling appropriate coalition participation**
- **Not all technologies required to implement cross-domain solutions exist today**
- **R&D initiatives should focus on these needed technologies:**
 - ✓ **Innovative approaches involving metadata tags;**
 - ✓ **Automated policy rule implementation;**
 - ✓ **Email file transfer across guards;**
 - ✓ **Collaboration and discovery;**
 - ✓ **Cross-domain access and Multi-Level Security**
- **Data ontology/schema agreements should be created within communities of interest, including most likely coalition partners**

Integrity - Service - Excellence

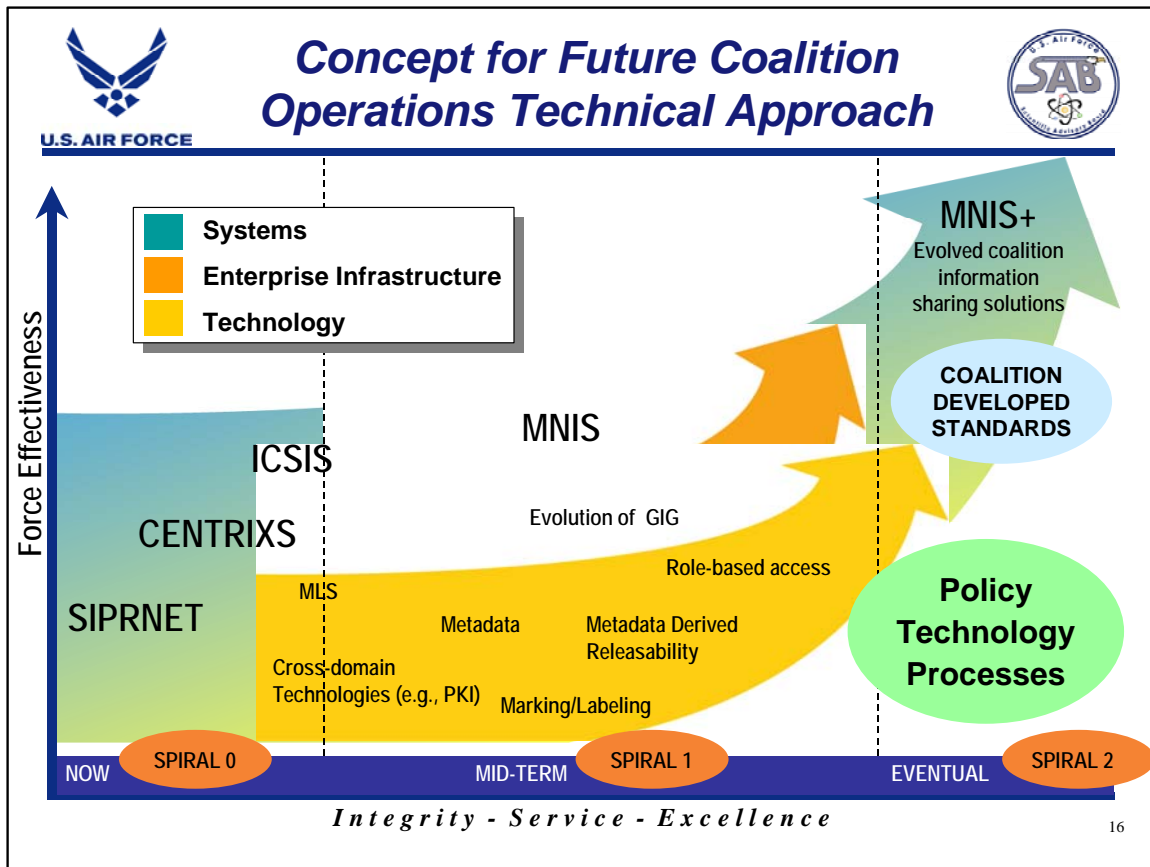
15

In order to achieve our concept of future coalition operations, we need to invest in new technologies.

The key technology needed, trusted cross-domain security solutions, will be dependent on MDR. This will enable appropriate and effective coalition participation. We do not have these technologies available today, so we propose an essential series of R&D initiatives coordinated and collaborated across the DoD and coalition community, particularly in the areas of metadata tagging.

In particular, we need guards to ensure metadata validity and security; automated rules and email filtering using guards; collaboration and discovery; and cross-domain access. While metadata tags are indeed very promising, we must note that particular attention should be paid early to implementation issues and the maintenance burden of a large scale, metadata-tagged system.

We also need to develop data ontology and schema agreements within the communities of interest and in this case we explicitly mean likely coalition partners.



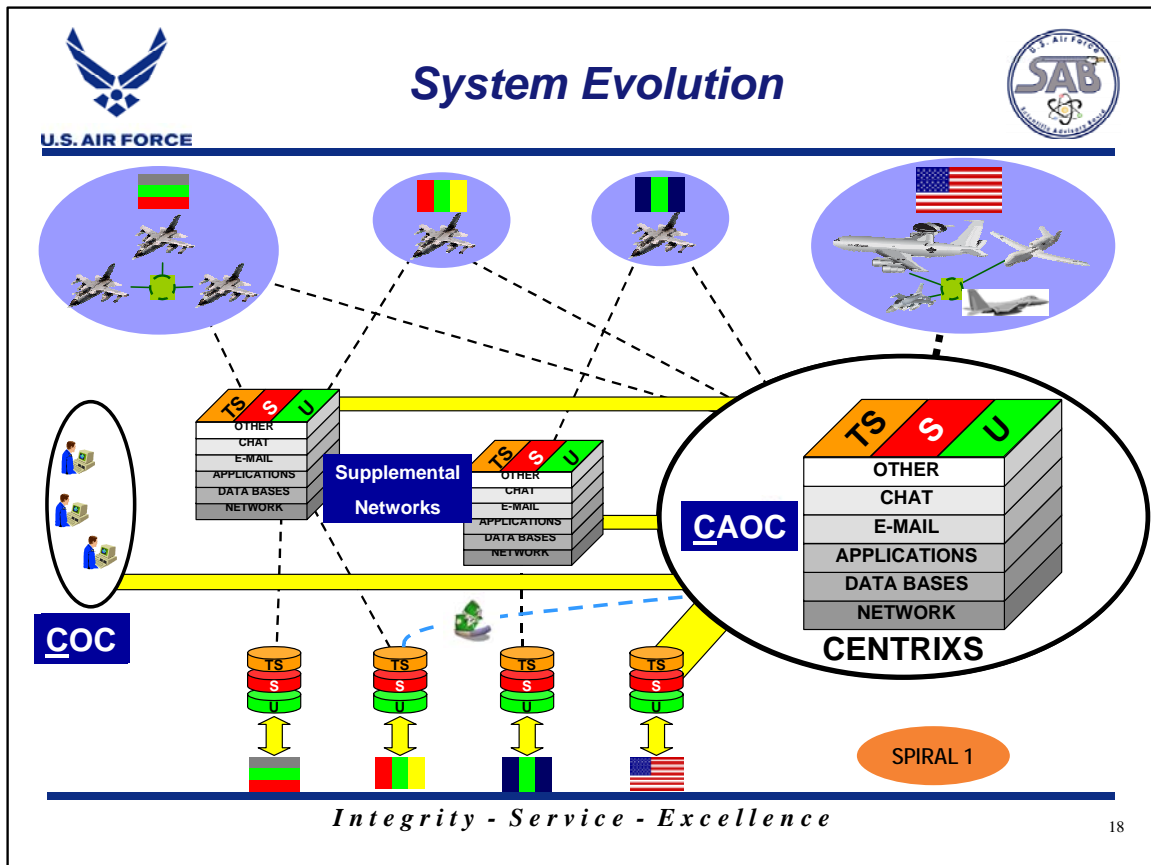
Here is a pictorial view of the technological path forward. We define three spirals.

Spiral 0 reflects work, under the auspices of the Office of the Assistant Secretary of Defense for Networks and Information Integration (ASD/NII), to make CENTRIXS and other coalition networks effective operational planning and execution systems. We suggest that concepts, architectures, and approaches used in ICSIS can be inserted into the CENTRIXS evolution process to enhance its functionality and, more importantly, the certifiability of the resultant networks.

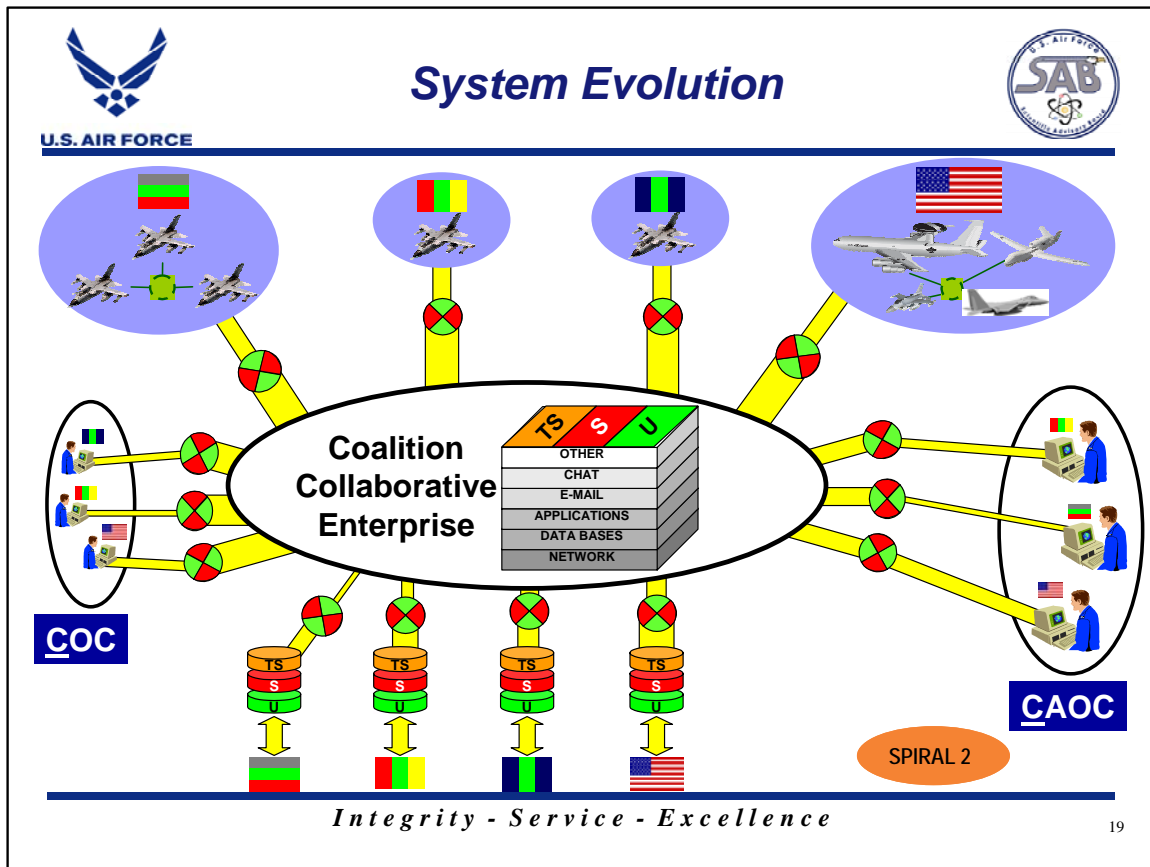
In Spiral 1 we see an initial rendition of a true multi-national information system (MNIS), which can be based on the current (single domain) ICSIS architecture. We envision this to be certified by the National Security Agency and appropriately accredited to handle the required security levels. Technology advances that will enable this include metadata tagging, Public Key Infrastructure, and security policy changes.

As we move forward into Spiral 2, we foresee an evolved MNIS with role-based access to information based on a fully functional MDR-based information distribution and collaboration network.

PUBLIC RELEASE AUTHORIZED





The transition to Spiral 1 will move all planning and mission execution elements from SIPRNET onto CENTRIXS, which will be connected to U.S. and coalition data sources, as well as other supplemental coalition networks.



19

The development and implementation of a system based on MDR will allow for the establishment of a Coalition Collaborative Enterprise, our envisioned Spiral 2. In this Spiral, releasable data will flow from U.S. and coalition partners into a common enterprise database. Because the data are meta-tagged, participants in the CAOC and higher-level Coalition Operations Centers (COC) will now be able to access available data based on a similar set of rules. These rules will be based on each individual's role in the operation and can be changed to match the operation and the Commander's intent. No longer will access to information be based solely on network access. Security guards will insure that only releasable meta-tagged data is allowed to flow into the database of the Coalition Collaborative Enterprise.



Recommendations – Training

Establish a comprehensive coalition training and exercise program that fully integrates coalition partner nations on a routine basis

- Coalition exercises should reflect combat realities; avoid “dumbing down” to accommodate policy and system constraints
- Exercises should optimize use of both U.S. and coalition partners’ operational capabilities
- U.S. forces and likely coalition partners should routinely train together to build trust
- Ensure that Blue Flag, Virtual Flag, Red Flag, constructive M&S, DMOC, and “live fly” correctly emulate how the coalition will fight

Integrity - Service - Excellence



20

With regard to training, we believe this is a vitally important issue and we recommend that the Air Force establish a comprehensive coalition training and exercise program. Coalition is the key word here. Partner nations should be fully and routinely integrated into this program, and these programs should not be “dumbed down” in order to meet policy and system constraints on non-U.S. participation. Effective training, which reflects combat realities, is not possible if coalition partners are denied access to our CAOCs because they contain classified U.S. information, and then, in lieu, are provided artificial data.

We believe that exercises need to include a full range of intelligence, surveillance, and reconnaissance (ISR) as well as all the other operational capabilities that the coalition will employ in real wartime.

U.S. forces ought to routinely train with likely coalition partner nations. This is as much to build trust, as it is to build capability. The Air Force’s training regimen should be tailored for not just U.S. Forces alone, but also for our likely coalition partners in collaboration with our own forces.

Finally, the major training mechanisms listed should correctly emulate how the coalition will fight. That is, the forces involved should “train as they will fight.”



Recommendations – Operational Capabilities

Designate the “CAOC as a weapon system”

- Establish coalition interoperability as a KPP for the Falconer Weapon System
- Provide coalition access to tools to enable collaborative planning
- Develop an architecture (operational, system, and technical views) that fully integrates coalition forces into the “networked force”
- Refine coalition operations through experiments
- Conduct realistic coalition exercises and training
- Formalize a requirement for an accredited content and role-based information system to support coalition operations

Integrity - Service - Excellence

21



With regard to operational capabilities, we recommend the Air Force put the “C” in “CAOC as a weapon system;” that is, make the AOC a true Coalition Air Operations Center.

To accomplish this we recommend coalition interoperability KPPs be established for the Falconer Weapon System. Currently, coalition capability in that weapon system is an afterthought. It is not a priority.

We recommend that coalition partners be provided access to tools that enable collaborative planning through the CAOC.

Furthermore, the Air Force should develop an architecture in collaboration with our coalition forces that allows us to interoperate effectively together. As stated previously, we assert again, here, that we need to experiment, conduct exercises, and training as a coalition force.

Finally, we should formalize a requirement for an MDR-based, accredited content and role-based information system to support coalition operations of the future.



Recommendations - Technology

Aggressively promote and influence multi-agency system developments essential to effective coalition operations

- ✓ Engage likely coalition partners to develop and evolve coalition network capabilities and classification systems to include:
 - ✓ Rule-based access, metadata tagging, marking/labeling
- ✓ Develop technologies and evolve a set of standardized cross-domain solutions (e.g., guards) that provide a rich set of services to enhance coalition operations to include:
 - ✓ Chat, whiteboard, e-mail, XML, structured data, voice-over IP, file sharing, web services, PKI, directory, search, video

Integrity - Service - Excellence



22

With respect to technology, we believe that the Air Force should do everything it can to promote and influence multi-agency development of the technologies that are necessary to achieve true coalition operations along the lines we have previously identified.

We need to encourage and engage likely coalition partners to develop and evolve networking capabilities and classification systems.

We should develop the technologies mentioned earlier and evolve a set of standardized cross domain solutions (i.e. guards) that move from today's manual and personnel-intensive transfer mechanisms (e.g., FDOs) to an environment that provides a rich set of services to include chat, whiteboard, e-mail, XML, structured data, voice-over-IP (voice over the Internet protocol, versus, for example, over telephone cables), file sharing, web services, PKI, directory, search, and video.

To achieve our end state we need to assure development of the technologies that enable MDR.



Recommendations - Systems

Establish a distributed coalition network environment that will enable and encourage coalition nations to develop interoperable C2 systems

- **Spiral 0**
 - ✓ Task an international working group to define standards and a roadmap for open architectures and information sharing among coalitions
 - ✓ Get off SIPRNET-based AOC by reconfiguring all AOC efforts into CAOC with a coalition-friendly CENTRIXS-like network
- **Spiral 1**
 - ✓ Build and implement systems to accommodate “Coalition Releasable” security domain
 - ✓ Establish a multi-national information sharing system evolved from the ICSIS services, certified by NSA, and appropriately accredited
- **Spiral 2**
 - ✓ Incorporate Metadata Derived Releasability technology into all systems

Integrity - Service - Excellence

23

With respect to systems, we need to define system level advances that incrementally move through Spiral 0 to Spiral 1 to Spiral 2.

As a first step today, the Air Force should set the objective of getting off the SIPRNET-based AOC configuration by moving AOC applications as soon as possible into a CAOC configuration using coalition friendly CENTRIXS-like networking, such as is being done today at Al Udeid. In addition, to begin to set the foundation for Spiral 2, an international working group must define standards and a roadmap for information sharing among coalition partners.³

To be sure, as we said, efforts along this path are already under way, but they need to be focused, enabled, and enhanced.

³ For this working group, each participating country (not necessarily limited to alliance countries) could be tasked with providing industrial representatives who were design engineers to an international working group. The group would be collocated and devote full-time effort over a one-year timeframe to define a design solution wherein each country could independently build conforming products. The resultant design could then be incorporated as a standard and distributed among any who wished to define compatible C2 systems.

In today's web-based environment, many candidate commercial products and standards could be reasonably assembled into a straw configuration suitable for allowing common coalition networking standards to be baselined. It would then be the task of our proposed working group to come up with a compatible set of standards and to define a compatibility test suite to enable multiple countries/companies to build compatible products.

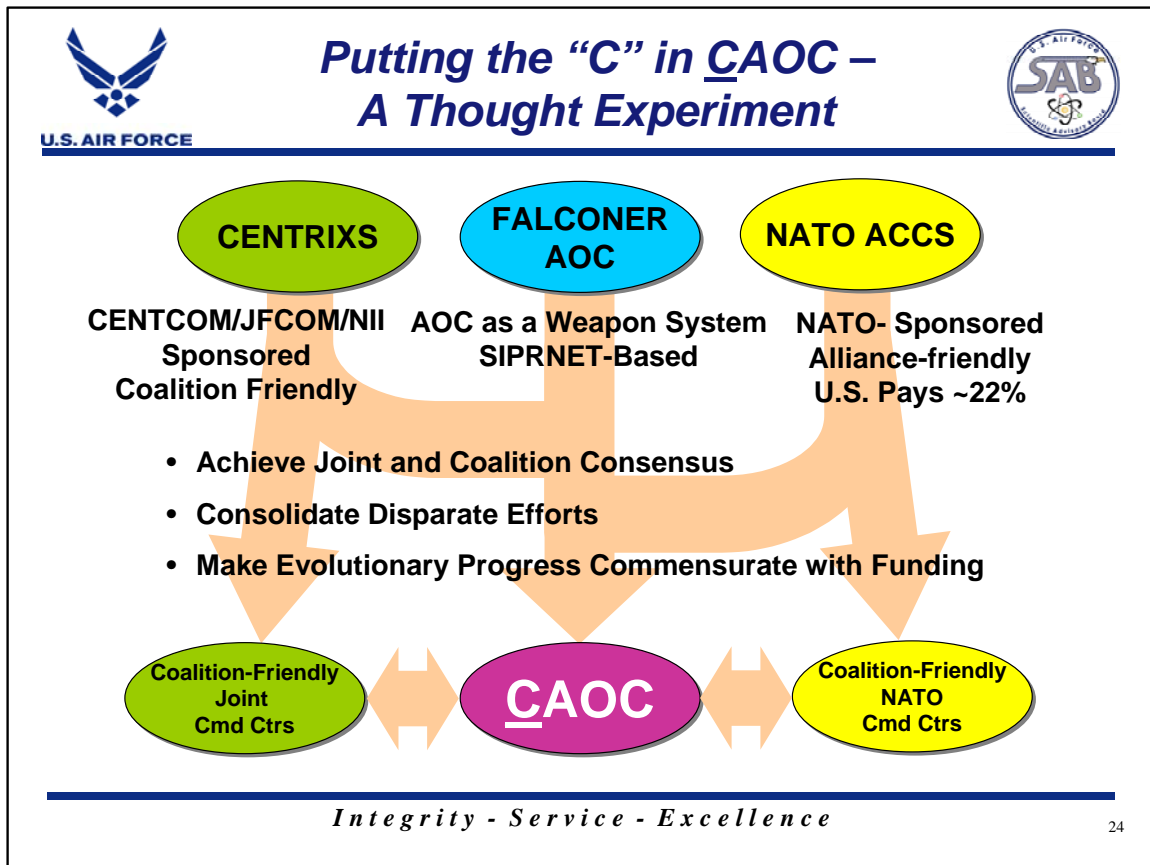
PUBLIC RELEASE AUTHORIZED

In Spiral 1 the Air Force should establish a coalition releasable security compartment, and establish a multi-national information service using ICSIS services capabilities as a model.

The Air Force also should shift its thinking and CONOPS from a U.S./Joint mentality to a coalition mentality.

Finally, in Spiral 2, we need to implement the MDR concept that we have spoken about, and we need to implement the Commanders' intent though near real time, machine-to-machine implementation of rule-based information access.

PUBLIC RELEASE AUTHORIZED



To conclude, we offer a "thought experiment" as to how the Air Force might choose to proceed to implement the recommendations the study proposes.

There are currently three significant broad, network-related initiatives. First, the FALCONER program is establishing the AOC as a weapon system. Second, various coalition networks are being integrated, and moved toward standardization under the CENTRIXS banner. Finally, the U.S. is funding about twenty-two percent of the NATO-sponsored Air Command and Control System (ACCS).

The Air Force could choose to actively influence the coordination and consolidation of these three paths to ensure a focused, coordinated joint and coalition (in this case, NATO) effort to build truly coalition friendly and compatible networking capabilities in each of these three major areas. In this manner, the Air Force could create an Air Force CAOC. Such a system could then serve as the basis for coalition-friendly Joint Command Centers and coalition-friendly NATO Command Centers, both of which, being built on similar architectures and along similar standards, would then be able to communicate with each other and with Air Force CAOCs. In doing so, it is likely that redundant and conflicting efforts could be reduced or eliminated, thereby saving money, which could be applied to accelerate the progress toward a truly effective and coalition-friendly Spiral 3 system implemented in all three areas.



Put the C in CAOC As a Weapons System

Integrity - Service - Excellence

25

Appendix A: Terms of Reference
USAF Scientific Advisory Board 2004 Summer Study

NETWORKING TO ENABLE COALITION OPERATIONS

Terms of Reference

Background

The US Air Force has begun migration toward a network-enabled force. Previous SAB Studies have suggested both the path toward, and the benefits of, this transformational change in warfare. At the same time, coalitions have become increasingly important in warfare for political, access, and other reasons. However new systems and technologies that enable networked operations are not always available and are often unaffordable to coalition partners, and, as a result, US Air Force and allied/coalition partner systems are diverging technologically. Instituting coalition net centric operations will require the mixing and matching of diverse systems to achieve desired capabilities. This can be achieved through appropriate data links, proper allocation of tasks to different systems of coalition partners that exploit the capabilities of their systems, the use of the network to compensate for inadequacies of participating systems, and the use of collaborative systems among coalition command centers. Multi-level security must also be addressed. Networked forces need to be designed to reduce the gap between the “haves” and the “have-nots” and provide a more effective total force.

Study Products

Briefing to SAF/OS & AF/CC in October 2004. Publish report in December 2004.

Charter

The study should identify and provide recommendations on the following issues:

- Operational Concept(s) for a networked coalition
- A roadmap for integrating or federating US and ally/coalition partner systems into a Net Centric system-of-systems and for enhancing collaboration
- A set of high payoff opportunities for enhancing interoperability while maintaining a proper level of security among component systemsSuggested technology releasability guidelines for classes of potential coalition partners

Scope Limitations

Because of the potentially large numbers of coalition partners, and the uniqueness of each one, this study could easily exceed the bounds of what the SAB is capable of completing as a summer study. Therefore the study should not attempt to address the issue for every coalition partner, but only for a small representative set of specific countries.

PUBLIC RELEASE AUTHORIZED

(This Page Intentionally Left Blank.)

PUBLIC RELEASE AUTHORIZED

Appendix B: Study Members

Study Leadership

Mr. Howard K. Schue – Chair
Dr. Peter R. Worch – Vice Chair
Dr. Alex Levis – Senior Civilian Participant
Brig Gen William Holland – General Officer Participant

Requirements, Operational Concepts, and Operational Architectures Panel

Maj Gen (Ret) John W. Hawley, USAF – Panel Chair
Mr. Timothy M. Bonds
Lt Gen (Ret) Lincoln D. Faurer, USAF
Dr. Janet Fender (Civilian Participant)
Maj Gen (Ret) George B. Harrison, USAF
Maj Mike Walker, USAFR – Panel Executive Officer
Maj Helen Meisenholder, USAF – Panel Technical Writer

Technology, Technology Architectures, and Acquisition Panel

Dr. Llewellyn S. “Doc” Dougherty – Panel Chair
Mr. Edward Brady
Mr. Scott Fouse
Maj Gen (Ret) Eric B. Nelson, USAF
Dr. William R. Swartout
Dr. Lionel Tiger
Capt Eve M. Burke, USAF – Panel Executive Officer
Maj Jeff Humphries, USAF – Panel Technical Writer

Standards, Releasability, Language, and Security Panel

Dr. Louis S. Metzger – Panel Chair
Maj Gen (Ret) John P. Casciano, USAF
Dr. Stephen E. Cross
Dr. Ray O. Johnson
Mr. James Shields
Maj Ronjon Annaballi, USAF – Panel Executive Officer
Capt Cicely Levingston, USAF – Panel Technical Writer

Roadmap and Implementation Panel

Mr. Thomas F. “Skip” Saunders
Dr. Ronald P. Fuchs
Dr. James B Peterson
Lt Gen (Ret) Stephen B Plummer, USAF
Dr. Robert W. Selden
Mr. Philip L. Soucy
Dr. Greg L. Zacharias
Capt Mike Bucher, USAF – Panel Executive Officer
Maj Timothy J. Landvogt, USAF – Panel Technical Writer
Mr. Mickey Schmidt - Multimedia

Study Management

Maj Christopher Berg, USAF – Study Project Manager
Maj Robert Renfro, USAF – Study Technical Writer
Mr. Paul Hazell – Study Technical Editor

PUBLIC RELEASE AUTHORIZED

(This Page Intentionally Left Blank.)

PUBLIC RELEASE AUTHORIZED

Appendix C: Visits and Briefings

Department of Defense

Under Secretary of Defense (Policy) – International Security Programs Office of National Disclosure Policy
Assistant Secretary of Defense/ Network Interoperability and Integration
Joint Chiefs of Staff Director of Command, Control, Communications, and Computer Systems
Office of Force Transformation
Defense Information Systems Agency
Defense Information Systems Agency Security Accreditation Working Group

U.S. Combatant and Regional Commands

U.S. Central Command
U.S. European Command
U.S. Joint Forces Command
U.S. Northern Command/ North American Air Defense
U.S. Pacific Command
U.S. Southern Command
U.S. Forces Korea
Joint Inter-Agency Task Force- South

Headquarters Air Force

Vice Chief of Staff of the Air Force
Air Force Chief Information Officer
Deputy Chief of Staff of the Air Force Air and Space Operations
▪ Deputy Chief of Staff of the Air Force Air and Space Operations Requirements Directorate
Deputy Chief of Staff of the Air Force Air and Space Operations
Deputy Under Secretary of the Air Force (International Affairs) Foreign Disclosure and Technology Transfer Division
Air Force Command, Control, Intelligence, Surveillance, and Reconnaissance Center
Task Force Enduring Look

Air Force Major Commands

Air Combat Command
Air Force Material Command
Air Force Space Command
Air Force Special Operations Command (point paper)
Pacific Air Forces
U.S. Central Command Air Forces

Combat Air Forces and Other Air Forces

16th Air Force
32nd Air Operations Group
Air Warfare Center
▪ RED FLAG
▪ BLUE FLAG
▪ DMOC (VIRTUAL FLAG)
Air Force Research Laboratories
Air Force Electronic Systems Command

Department of Homeland Security

U.S. Coast Guard

Department of State

Bureau of Political Military Affairs – Office of Regional Security and Arms Transfers

Intelligence Community

Defense Intelligence Agency

Intelligence Community Chief Information Officer

National Reconnaissance Office

National Security Agency

Foreign Governments and NATO

Australian Department of Defense

- Defense Science and Technology Organization

Defense Attaché Office of Australia

Defense Attaché Office of Chile

Defense Attaché Office of Ghana

Defense Attaché Office of India

Denmark (at RED FLAG)

Singapore (at RED FLAG)

Spain (at USCENTCOM)

Swedish Ministry of Defense

UK Royal Air Force Strike Command

UK (at RED FLAG)

North Atlantic Treaty Organization – Air Command and Control System

North Atlantic Treaty Organization – Allied Command Operations

North Atlantic Treaty Organization – Allied Command Transformations

North Atlantic Treaty Organization – NATO Consultation, Command and Control Agency

Appendix D: Acronyms and Abbreviations

ACCS	Air Command and Control System
AF/XI	Deputy Chief of Staff of the Air Force Warfighting Integration
AF/XO	Deputy Chief of Staff of the Air Force Air and Space Operations
AOC	Air Operations Center
AOR	Area of Responsibility
ASD/NII	Assistant Secretary of Defense for Network Interoperability and Integration
ATO	Air Tasking Order
C2	Command and Control
CAOC	Combined Air Operations Center
CBIS	Content Based information Security
CENTRIXS	Combined Enterprise Regional Information Exchange System
CFACC	Combined Forces Air Component Commander
COC	Coalition Operations Center
CONOPS	Concept of Operations
CSAF	Chief of Staff of the Air Force
DAA	Designated Accreditation Authorities
DCFACC	Deputy Combined Forces Air Component Commander
DISN	Defense Information System Network
DMOC	Distributed Mission Operations Center
DMOC	Distributed Mission Operations Center
DoD	Department of Defense
FDO	Foreign Disclosure Office or Foreign Disclosure Officer
GIG	Global Information Grid
IC	U.S. Intelligence Community
ICISIS	Intelligence Community System for Information Sharing
IP	Internet Protocol
ISR	Intelligence, Surveillance, and Reconnaissance
JCS	Joint Chiefs of Staff
JOC	Joint Operations Center
KPP	Key Performance Parameter
M&S	Modeling and Simulation
MAJCOMS	(Air Force) Major Commands
MDR	Metadata-Derived Releasability
MIDS	Multifunctional Information Distribution System
MLS	Multi-Level Security
MNIS	Multinational Information Sharing
MNIS	Multinational Information Sharing
MSL	Multiple Security Levels
NAF	Numbered Air Force
NATO	North Atlantic Treaty Organization
NSA	National Security Agency
OEF	Operation Enduring Freedom
OIF	Operation Iraqi Freedom
OSD	Office of the Secretary of Defense
PKI	Public Key Infrastructure
R&D	Research and development
SAF/AQ	Assistant Secretary of the Air Force (Acquisition)

PUBLIC RELEASE AUTHORIZED

SecAF	Secretary of the Air Force
SIPRNET	SECRET Internet Protocol Router Network
TCT	Time Critical Target or Time Critical Targeting
USCENTAF	U.S. Central Command Air Forces
USCENTCOM	U.S. Central Command
Voice over IP	Voice over Internet protocol
XML	Extensible Markup Language

PUBLIC RELEASE AUTHORIZED

PUBLIC RELEASE AUTHORIZED

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and manipulating the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget Paperwork Reduction Project (0704-0188), Washington, DC 20503.				
1. AGENCY USE ONLY (Leave Blank)		2. REPORT DATE 1 July 2004		3. REPORT TYPE AND DATES COVERED Final, January 2003 – July 2004
4. TITLE AND SUBTITLE <i>Networking to Enable Coalition Operations, Volume 1: Executive Summary and Annotated Brief (PR)</i>			5. FUNDING NUMBERS	
6. AUTHOR(S) Mr. Howard K. Schue, Dr. Peter R. Worch, Dr. Alex Levis, Brig Gen William Holland, USAF, Maj Gen (Ret) John W. Hawley, USAF, Mr. Timothy M. Bonds, Lt Gen (Ret) Lincoln D. Faurer, USAF, Dr. Janet Fender, Maj Gen (Ret) George B. Harrison, USAF, Dr. Llewellyn S. Dougherty, Mr. Edward Brady, Mr. Scott Fouse, Maj Gen (Ret) Eric B. Nelson, USAF, Dr. William R. Swartout, Dr. Lionel Tiger, Dr. Louis S. Metzger, Maj Gen (Ret) John P. Casciano, USAF, Dr. Stephen E. Cross, Dr. Ray O. Johnson, Mr. James Shields, Mr. Thomas F. "Skip" Saunders, Dr. Ronald P. Fuchs, Dr. James B Peterson, USAF, (Retired), Lt Gen (Ret) Stephen B Plummer, USAF, Dr. Robert W. Selden, Mr. Philip L. Soucy, Dr. Greg L. Zacharias				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) HQ USAF/SB 1180 AF PENTAGON RM 5D982 WASHINGTON, DC 20330-1180			8. PERFORMING ORGANIZATION REPORT NUMBER SAB-TR-04-01	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) SAF/OS, AF/CC AIR FORCE PENTAGON WASHINGTON, DC 20330-1670			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES				
12a. DISTRIBUTION/AVAILABILITY STATEMENT Approved for Public Release			12b. DISTRIBUTION CODE Distribution Statement A	
ABSTRACT (Maximum 200 Words) <i>Networking to Enable Coalition Operations:</i> In the past four decades, the United States has been the predominant force in peacekeeping, peacemaking, and combat operations in which it has participated. Two changes are now being experienced. First, post-Cold War contingencies and the Global War on Terrorism have illustrated the increasing importance of constructive coalition relations. Second, as U.S. forces become more network-centric, effective integrated operations with coalition partners are becoming increasingly difficult and dependent upon the ability to share information electronically. In particular, the dynamic nature of air operations demands rapid transfer of data among the forces. However, security concerns prevent full (and often, even partial) access to our networks by others. While workarounds have been implemented, sometimes with excellent combat results, this limited access has impaired the ability of U.S. Forces to truly exploit the diverse capabilities of coalition partners and perhaps reduce our Operations Tempo. This Study addresses the issue of networking for coalition air operations from policy, operational, and technical viewpoints and concludes that improvements in all three areas are essential to effective coalition air operations. The Air Force can take unilateral action to further developments, designate the CAOC as a weapon system, foster demonstrations and experiments to explore CAOC solutions, and improve training and exercises. It can also encourage OSD and Joint levels to review and revise national disclosure policies.				
14. SUBJECT TERMS AOC, CAOC, CENTRIXS, Coalition, Disclosure, ICSIS, Metadata-Derived Releasability, Multinational, Multi-Level Security, Multiple Security Levels, NECO, Need to Know, Need to Share, Networking, Multi-National Information Sharing, FALCONER			15. NUMBER OF PAGES 40	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT UNCLASSIFIED	

PUBLIC RELEASE AUTHORIZED

